PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, G06K 9/00

A1

(11) International Publication Number: WO 00/26749

(43) International Publication Date: 11 May 2000 (11.05.00)

(21) International Application Number: PCT/US99/25375

(22) International Filing Date: 28 October 1999 (28.10.99)

(30) Priority Data:
09/185,380 3 November 1998 (03.11.98) US

(71) Applicant *(for all designated States except US)*: DIGIMARC CORPORATION [–/US]; Suite 500, One Centerpointe Drive, Lake Oswego, OR 97035–8615 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: DAVIS, Bruce, L. [–/US]; 15599 Village Drive, Lake Oswego, OR 97034 (US). PERRY, Burt, W. [–/US]; 8145 SW Barnard Drive, Beaverton, OR 97007 (US). CARR, J., Scott [–/US]; 7814 SW 189th Avenue, Beaverton, OR 97007 (US). SHAW, Gilbert, B. [–/US]; 13025 SW Park Way, Portland, OR 97225 (US). RHOADS, Geoffrey, B. [–/US]; 304 SW Tualatin Loop, West Linn, OR 97068 (US).

(74) Agent: CONWELL, William, Y.; Digimarc Corporation, Suite 500, One Centerpointe Drive, Lake Oswego, OR 97035–8615 (US).

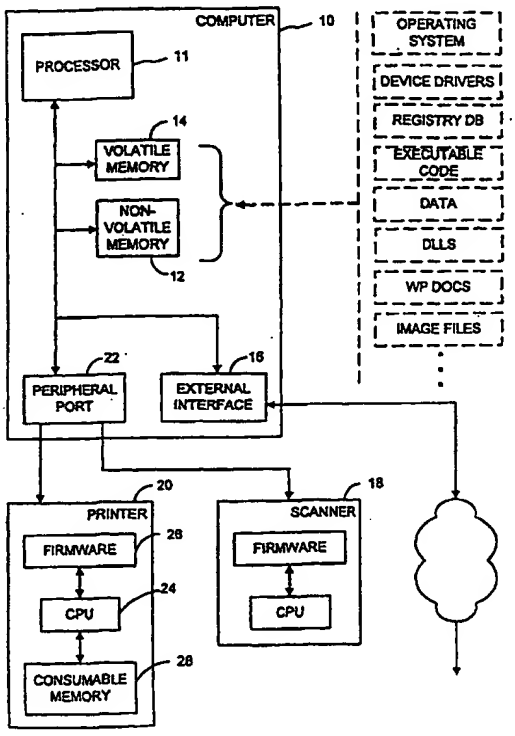
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND SOFTWARE FOR EVIDENCING ILLICIT USE OF A COMPUTER SYSTEM

(57) Abstract

A computer (10) is provided with software that looks for certain activities that may be illicit (e.g. processing of a graphic file corresponding to a banknote). If such an activity is detected, tracer data detailing the activity is generated and secretly stored in the computer (10). If the computer (10) is later searched or seized, the tracer data can be recovered and employed as evidence of the computer's use, e.g. in counterfeiting. To detect whether graphic image data corresponds to a banknote, two analysis techniques may be used. One is based on detection of a visible pattern characteristic of a security document. The other is based on detection of a steganographic digital watermark characteristic of a security document. If either characteristic is found, the image is flagged, and appropriate anti–counterfeiting steps may be taken. Detection of the visible pattern can be performed using a series of successively more rigorous tests. If the image fails the first test, successive tests can be skipped, speeding the process. Hough transform–based pattern recognition techniques are used in some embodiments. Provision of both a visible pattern detector and a watermark detector in a single apparatus enhances reliability, while permetting various implementation efficiencies.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND SOFTWARE FOR EVIDENCING ILLICIT USE OF A COMPUTER SYSTEM

Field of the Invention

The present invention relates to computer systems, and more particularly relates to techniques for establishing persistent evidence of a computer's use for possibly illicit purposes (e.g. counterfeiting).

Background and Summary of the Invention

Fifty years ago, counterfeiting was a rare art practiced by a small number of skilled engravers using esoteric equipment. Today, counterfeiting is a rampant problem practiced by thousands of criminals using ubiquitous computer equipment.

Statistics from the U.S. Secret Service illustrate the magnitude of the problem in the United States. In a recent report, the Secret Service stated:

> The amount of counterfeit currency passed in the United States over the last three fiscal years has remained fairly consistent; however, 1998 has seen a significant increase, largely due to inkjet produced counterfeits. Inkjet produced counterfeit currency comprised only 0.5% of the total counterfeit currency passed in fiscal year 1995. In comparison, 19% of the total counterfeit currency passed in the United States during fiscal year 1997 was inkjet produced, and 43% of the counterfeit currency passed through August 1998 has been ink jet counterfeit currency.
>
> This trend is attributed to rapid improvements in technology, and the ever-increasing availability and affordability of scanners, high-resolution inkjet and other output devices, and computer systems. Digital counterfeiting is likely to continue to increase as the capabilities of systems and devices continue to improve, and as these capabilities become more readily understood by the criminal element.

Accompanying the Secret Service report was a table identifying the number of domestic counterfeiting plants raided, by type. Again, the explosive growth of inkjet counterfeiting is evident:

Type of Counterfeiting Plant	FY95	FY96	FY97	FY98 (through July)
Offset Counterfeiting	60	29	23	10
Toner-Based Counterfeiting	59	62	87	47
Inkjet-Based Counterfeiting	29	101	321	477

The problem is not limited to the United States; statistics from other countries show the above-detailed trends are worldwide.

Various means have been deployed over the years to deter the counterfeiting of banknotes and similar financial instruments. One is to incorporate design features in banknotes that are difficult to replicate. Another is to equip color photocopiers with the capability to recognize banknotes. If such a photocopier is presented with a banknote for duplication, copying is disabled or impaired.

Yet another approach is for color photocopiers to imperceptibly write their serial number on all output sheets, e.g. using small, light yellow lettering. (Such an arrangement is shown, e.g., in European laid-open application EP 554,115 and in U.S. patent 5,557,742.) While unknown to most of the public, the majority of color photocopiers employ this, or similar means, to mark all output copies with covert tracing data.

The inclusion of covert tracing data in all printed output from color photocopiers (and some color printers) brings into play the balancing of law enforcement needs versus the widely recognized users' rights of privacy and freedom of expression. Unbounded use of such covert marking techniques can raise the spectre of an Orwellian "Big Brother."

In accordance with a preferred embodiment of the present invention, tracer data is selectively generated to assist law enforcement agencies in prosecuting counterfeiters. However, instead of rotely incorporating such data into all printed

output, it is secretly stored in the counterfeiter's computer. If the computer is later searched or seized, the tracer data can be recovered and employed as evidence of the computer's use in counterfeiting.

The foregoing and additional features and advantages of the present invention will be more readily apparent from the following detailed description, which proceeds with reference to the accompanying drawings.

Brief Description of the Drawings

Fig. 1 is a diagram of a computer system according to one embodiment of the present invention.

Fig. 2 is a diagram illustrating certain of the principles used in the Fig. 1 embodiment.

Detailed Description

Referring to Fig. 1, a computer system 10 employed in one embodiment of the present invention includes a processor 11, a non-volatile store 12, volatile memory 14, an external interface 16, and various peripherals (e.g. a scanner 18, a printer 20, etc.).

The processor 11 typically comprises a CPU, such as one of the microprocessors available from Intel, Sun, AMD, Cyrix, Motorola, MIPS, etc. Alternatively, the processor can take other forms, including hardwired logic circuitry, programmable logic (e.g. FPGAs), or yet-to-be-devised processing arrangements.

The non-volatile store 12 typically comprises a magnetic disk, but can also include other writeable media, including optical disks, flash memory, EEPROMS, ROMBIOS, etc. The non-volatile store can be physically located with the processor 11 (e.g. hard disk, CMOS memory with system setup data, etc), and/or can be remote (e.g. a networked drive, storage accessible over the Internet, etc.).

The volatile memory 14 typically comprises RAM, either integrated with the CPU (e.g. cache), and/or separate.

The external interface 16 can take various forms, including a modem, a network interface, a USB port, etc. Any link to a remote resource other than common peripherals is generally considered to employ an external interface.

Stored in the non-volatile store 12 is various software. This includes operating system software, applications software, and various user files (word processing documents, image files, etc.). The operating system software typically includes a thousand or more files, including a registry database (detailing the resources available in the system, etc.) and various device drivers (which serve as software interfaces between the CPU and peripheral devices, such as scanner 18 and printer 20). The applications software includes executable code and data. Both the operating system software and the applications software may employ shared files (e.g. DLLs) which can be utilized by different executables and/or operating system components to provide desired functionality.

While illustrated as resident in the non-volatile store 12, the foregoing software is generally loaded into the volatile memory 14 for execution.

The peripherals 18, 20 are typically connected to the computer system through a port 22 (e.g. serial, parallel, USB, SCSI, etc.) which permits bi-directional data exchange. Each peripheral typically includes its own processor circuitry 24 that operates in conjunction with firmware 26 (software resident in memory within the printer) to perform peripheral-specific processing and control functions. In addition to the memory in which the firmware is stored (e.g. EEPROM, flash memory, etc.), some peripherals have other data storage. For example, the disposable "consumables" in printers increasingly include their own non-volatile memories 28 in which various calibration and/or usage data is stored.

In one embodiment of the present invention, the computer system writes forensic tracer data (sometimes terms an "audit trail") to a non-volatile store if it detects a possibly illicit action, e.g. the processing of image data corresponding to a banknote. (For expository convenience, the term "banknote" is used to refer to all manner of value documents, including paper currency, travelers checks, money orders, stamps, university transcripts, stock certificates, passports, visas, concert- or sporting event tickets, etc.) The data is written in a manner(s), and/or to a location(s), chosen to minimize its possible detection by a cautious perpetrator. If the computer is later inspected pursuant to a lawful search and seizure, it can be analyzed for the presence of incriminating tracer data.

There is considerable prior work in the field of detecting security documents from image data. Published European application EP 649,114, for example, describes banknote detection techniques based on the use of fuzzy inferencing to detect geometrical arrays of certain patterns that are characteristic of banknotes. U.S. patents 5,515,451, 5,533,144, 5,629,990, and 5,796,869 describe banknote detection techniques based on different pattern matching techniques (e.g. to recognize the Federal Reserve seal). Xerox has also proposed its data glyph technology (detailed, e.g., in U.S. patents 5,706,364, 5,689,620, 5,684,885, 5,680,223, 5,668,636, 5,640,647, 5,594,809) as a means to mark security documents for later machine-identification.

Another means for detecting security documents is by use of Hough-based pattern matching techniques as described, e.g., in Hough's U.S. patent 3,069,654, and Ballard, "Generalizing the Hough Transform to Detect Arbitrary Shapes," Pattern Recognition, Vol. 13, No. 2, pp. 111-122, 1981. One embodiment of such a system follows the approach outlined in the Ballard paper, and employs plural tables corresponding to different patterns found on banknotes, with different confidence. Gross Hough processing is first performed using one or more rotationally-invariant features (e.g. U.S. Federal Reserve Seal) to quickly identify most image sets as not banknote-related. Any data that looks to be potentially bank-note related after the first check is subjected to successively more selective, higher-confidence tests (some stepping through plural rotational states) to weed out more and more non-banknote image sets. Finally, any image data passing all the screens is concluded to be, to a very high degree of certainty, a banknote. An appropriate signal is then generated (e.g. a change in state of a binary signal) to indicate detection of a banknote.

Neural networks and algorithms are also suitable for detection of patterns characteristic of banknotes, as illustrated by European patent EP 731,961, etc.

In the present assignee's prior applications (e.g. 08/649,419, 09/074,034, 09/127,502, 60/082,228; corresponding to PCT applications US99/08252 and US99/14532) techniques are disclosed for marking security documents with generally imperceptible, or steganographic, watermark data, so as to facilitate later identification of such documents. By employing digital watermark-based banknote detection in

combination with visible feature-based banknote detection, very high confidence recognition of banknote data can be achieved.

The artisan is presumed to be familiar with the various approaches for recognizing banknotes from image data, of which the foregoing is just a sampling.

While such banknote-detection techniques are commonly implemented in resource-intensive form, using sophisticated processing units (e.g. the main CPU of a copier), this need not be the case. To reduce the resource requirements, the detection algorithm can be tailored to operate on parts of scan-line data, without buffering the entire set of image data for analysis. The algorithm can be implemented on less-sophisticated processors, such as those used in the scanner 18 or the printer 20. The processors can be programmed, by appropriate firmware, to perform such processing on any image data scanned by, or printed by, such devices. And as modems and other interfaces (SCSI, FireWire, IDE, ATAPI, etc.) continue their evolution from dedicated hardware to software-based implementations, their data processing capabilities increase commensurately. Thus, for example, software-implemented modems, network interfaces, UARTs, etc., can monitor the data traffic passing therethrough and flag any that appears to be banknote-related. The full analysis operation can be performed by the interface, or the data can be copied and passed to the main processor for further analysis.

In the preferred embodiment of the present invention, when banknote image data is detected, storage of forensic data is triggered. The forensic data typically includes at least the date (and optionally the time) at which the possibly illicit action occurred. Additionally, the forensic data can include the file name of the banknote image data (if available), and a code indicating the nature of the event noted (e.g., banknote data detected by the printer; banknote data detected passing through the modem on COM2; banknote data detected written to removable media having volume ID 01FF38; banknote data detected in file opened by Adobe Photoshop, etc.) The forensic data can additionally detail the source from which the data came, and/or the destination to which it was sent (e.g. IP/email addresses). In operating systems requiring user login, the stored forensic data will typically include the use ID. System status data can also be included, e.g. identifying peripheral devices attached to the

system, code loaded into RAM memory, the amount of time the user spent working on the illicit data, etc. Selected data from any operating system registry database (e.g. identifying the registered owner of certain applications software then-loaded on the computer, software serial numbers, operational parameters, etc.) can likewise be included. If the computer is on a network or on the Internet, the network address, Ethernet MAC address, AppleTalk name and zone, TraceRoute information, or IP address information can be stored. If the illicit action has been detected by reference to a watermark or other embedded data, payload data recovered from the watermark can be included in the forensic tracer data.

On one extreme, the foregoing (and possibly more) information can be stored in detailed forensic tracer records. At the other extreme, the forensic tracer record can comprise a single bit indicating that the computer system has been used -- at least once -- for a possibly illicit action.

Expecting that savvy counterfeiters will attempt to defeat such forensic tracer data, such data is desirably generated, transmitted, and stored redundantly, transparently, and inconspicuously.

Redundant generation of the tracer data refers to detection of possibly illicit activity at various points in the computer system, and/or during various operations. Referring to Fig. 2, possibly illicit activity can be detected, e.g., during scanning of an image, printing of a document, receiving or transmitting a file through a modem connection, opening a file with an application program, saving a file with an application program, copying data to a clipboard, etc. By providing multiple opportunities for detection of possibly illicit activities, the robustness of the system is increased.

Redundant transmission of the tracer data refers to its transmission to storage media several times. When a possibly illicit activity is detected, it desirable to send tracer data to storage both immediately and on a delayed basis (e.g. five minutes after detection of banknote data, and every two minutes thereafter for a period of M minutes). By sending the data to storage repeatedly, the robustness of the system is again increased.

Redundant storage of the tracer data refers to its storage at several different locations (simultaneously or sequentially).

If even one instance of the redundantly generated/transmitted/stored tracer data survives the counterfeiter's attempts to redact incriminating data, it will be useful evidence in any prosecution.

Transparent generation/transmission/storage means that the acts associated with these operations will not arouse the counterfeiter's suspicion.

Various software tools are available to trace program execution. A savvy counterfeiter may employ such tools to monitor all disk writes performed by his system. Consider, for example, a counterfeiter using an image processing program in aid of his counterfeiting. The person may monitor the sequence of files opened and closed (and/or the data read/written) during use of the program for image processing with non-banknote data, and then be suspicious if different files, or in different orders, are opened and closed when performing the same image processing operations on banknote data. Thus, at least some of the forensic data should be stored using routine operations and routine files (e.g. writes to files that are used during normal program execution). Of course, such tracer data should be written in a manner assuring that the data will persist -- either in the location originally written, or by copying during subsequent machine operation (e.g. on closing the application program, shutting down the operating system, etc.) to a location assuring longer-term availability.

Program-tracing tools typically monitor just the computer's main CPU so -- where possible -- at least some of the tracer data should be stored under the control of a different processing element, or in a location to which the tool's capabilities do not extend. Another option is to keep at least some of the tracer data in RAM memory for a period after the illicit action has been detected, and store it later.

Yet another option is to store at least some forensic tracer records in the operating system registry database. This resource is commonly accessed during system operation, so references to the database may not give rise to suspicion.

Inconspicuous storage covers a wide range of options. One is that the data be encrypted. This assures that simple disk-scanning operations attempting to find byte strings likely associated with tracer data will be unsuccessful. (Numerous encryption techniques are known, e.g. RSA, PGP, various private key techniques, etc., any of which can be used.)

Encrypted tracer data can be stored with other encrypted system data, such as in a password file. Due to its encrypted nature, a hacker may not be able to discern what part of the stored data is tracer data and what part is, e.g., password data. Attempts to redact the tracer data risks corrupting the password data, jeopardizing the counterfeiter's later ability to login to the machine.

Another possibility is to steganographically encode the tracer data, e.g. by randomizing/obfuscating same and inconspicuously hiding it amidst other data (e.g. within graphic or audio files associated with start-up or shut-down of the computer operating system, or wherever else noise-like data can be introduced without alerting the user to its presence). Still another possibility is to create null code that resembles normal instructions or data, but instead serves as a forensic tracer record.

To avoid creation of telltale new files in the non-volatile memory, the tracer data can be patched into existing files, by appending to the end or otherwise. Or, rather than storing the tracer data as the content of a file, the data can be stored among a file's "properties."

Another way to avoid creating new files is to avoid using the computer's "file system" altogether, and instead use low-level programming to effect direct writes to typically-unused or reserved physical areas on the disk. By such techniques, the data is resident on the disk, but does not appear in any directory listing. (While such data may be lost if disk optimization tools are subsequently used, those skilled in the art will recognize that steps can be taken to minimize such risks.)

Yet another way to avoid creating new files is to relay at least some of the tracer data to outside the computer. One expedient is to use an external interface to transmit the data for remote storage. Again, a great variety of techniques can be employed to reliably, yet effectively, effect such transmission. And the data transmission need not occur at the moment the possibly illicit action is occurring. Instead, such data can be queued and relayed away from the machine at a later time.

Still another way to avoid creating new files is to make use of deadwood files that commonly exist on most computers. For example, application programs typically employ installation utilities which copy compressed files onto the disk, together with code to decompress and install the software. These compressed files and installation

programs are usually not deleted, providing opportunities for their use as repositories of tracer data. Similarly, many computers include dozens or hundreds of duplicate files – only one of which is commonly used. By converting one or more of these files to use as a repository for tracer data, additional inconspicuous storage can be achieved.

Some application programs include hundreds of files, various of which are provided just for the occasional use of the rare super-user. Files that pass some litmus test of inactivity (e.g. not ever used, or not accessed for at least two years) might serve as tracer data repositories. (Disk utilities are available to determine when a given file was last accessed.) Yet another option is to append data to an application's Help files, or other binary data files used to save program state information for the application.

Resort may also be made to various of the known techniques employed in computer viruses to generate, transmit, store and disseminate/replicate the forensic tracer data in manners that escape common detection. Moreover, such virus techniques can be used to initially spread and install the functionality detailed above (i.e. pattern recognition, and tracer data generation/transmission/storage) onto computers without such capabilities.

Some embodiments may perform self-integrity checks of old tracer records each time a new banknote is encountered, and repair any damage encountered. Similarly, old tracer records can be expanded to detail new illicit acts, in addition to (or in lieu of) creating independent records for each illicit act.

Various tools can be used to replicate/propagate forensic tracer records to further infest the system with incriminating evidence. Utility software such as disk defragmenters, disk integrity checks, virus checkers, and other periodically-executed system maintenance tools can be written/patched to look in some of the places where forensic tracer records may be found and, if any are encountered, copy them to additional locations. Similar operations can be performed upon termination of selected application programs (e.g. image processing programs).

The foregoing is just the tip of the iceberg. Those skilled in the arts of computer programming, operating system design, disk utilities, peripheral firmware development, packet data transport, data compression, etc., etc., will each recognize many different opportunities that might be exploited to effect surreptitious, reliable banknote detection,

and transmission, storage, and/or replication of tracer data. Again, if even one tracer record persists when the computer is searched by suitably-authorized law enforcement officials, incriminating evidence may be obtained. The high odds against ridding a computer of all incriminating data should serve as a deterrent against the computer's use for illegal purposes in the first place.

As noted, the computer system desirably includes several checkpoints for detecting illicit actions. In the case of banknote image processing, for example, detectors can be implemented in some or all of the following: in image processing software applications, in DLLs commonly used with image processing, in printer drivers, in printer firmware, in scanner drivers, in scanner firmware, in modem or other external interface drivers and software, in email software, in FTP software, in the operating system (looking at the clipboard, etc.), etc., etc. Similarly, where practical, the checking should be done by several different processors (e.g. main CPU, programmable interface chips, scanner microcontroller, printer microprocessor, etc.).

From the foregoing, it will be recognized that techniques according to the present invention can be used to discourage counterfeiting, and to aid in its prosecution when encountered. Moreover, this approach obviates the prior art approach of marking all color photocopies with tracer data, with its accompanying privacy and first amendment entanglements.

Having described and illustrated the principles of our invention with reference to an illustrative embodiment and several variations thereon, it should be recognized that the invention can be modified in arrangement and detail without departing from such principles.

For example, while the detailed embodiment has focused on a computer system, the same techniques can likewise be employed in stand-alone color copiers, etc.

Similarly, while the detailed embodiment has focused on counterfeiting, it will be recognized that computers can be employed in various other illicit or unauthorized activities. Each generally is susceptible to computer-detection (e.g. threats against the president may be detected by specialized natural language analysis programs; computer-aided synthesis of illegal drugs may be indicated by certain chemical modeling instructions in software specific to that industry; unauthorized duplication of

copyrighted works may be flagged by the presence of embedded watermark data in the copyrighted work; unauthorized distribution of classified or confidential business documents may be detected using known techniques, etc.). The storage of forensic tracer data along the lines detailed above is equally applicable in such other contexts.

In the future, support for illicit activity detection may be routinely provided in a wide variety of software and peripherals. In one embodiment, the software and peripherals may include generic services supporting the compilation of forensic tracer data, its encryption, transmission, storage, etc. These generic services can be invoked by detector modules that are customized to the particular illicit/unauthorized activity of concern. Some of the detector modules can be fairly generic too, e.g. generic pattern recognition or watermark detection services. These can be customized by data loaded into the computer (either at manufacture, or surreptitiously accompanying new or updated software) identifying particular images whose reproduction is unauthorized/illicit. As new banknotes are issued, updated customization data can be distributed. (Naturally, such detector customization data will need to be loaded and stored in a manner that is resistant against attack, e.g. using the approaches outlined above for the covert tracer data.)

While the invention is described in the context of an end-user computer, the principles are equally applicable in other contexts, e.g. in server computers. Moreover, the principles are not limited to use in general purpose personal computers but can also be applied in other computer devices, e.g. digital cameras, personal digital assistants, set-top boxes, handheld devices, firewalls, routers, etc.

Although not belabored above, it will be understood that law enforcement agencies will have software recovery tools that can be employed on suspect computer systems to recover whatever forensic tracer data may persist. Briefly, such tools know where to look for tracer data and, when encountered, know how to interpret the stored records. After analyzing the non-volatile stores associated with a suspect computer system, the recovery software will report the results. The implementation of such tools is well within the capabilities of an artisan.

While the foregoing disclosure has focused exclusively on the storage of forensic tracer data as the response to a possibly-illicit action, more typically this is just

one of several responses that would occur. Others are detailed in the previously-referenced documents (e.g. disabling output, hiding tracer data (e.g. as in patent 5,557,742, or using steganographically encoded digital watermark data) in the output, telephoning law enforcement officials, etc.).

To provide a comprehensive disclosure without unduly lengthening this specification, applicants incorporate by reference the patent applications and documents referenced above. By so doing, applicants mean to teach that the systems, elements, and methods taught in such documents find application in combination with the techniques disclosed herein. The particular implementation details of such combinations are not belabored here, being within the skill of the routineer in the relevant arts.

In view of the many possible embodiments in which the principles of our invention may be realized, it should be recognized that the detailed embodiments are illustrative only and should not be taken as limiting the scope of our invention. Rather, we claim as our invention all such modifications, combinations, and implementations as may come within the scope and spirit of the following claims, and equivalents thereof.

WE CLAIM:

1. A method for discouraging use of a computer system for an illicit activity, the system having associated therewith at least one data processor and at least one non-volatile data store, the method comprising:

receiving a signal indicating possible use of a system component for an illicit activity; and

in response to receipt of said signal, storing forensic tracer data in at least one of said non-volatile data stores;

wherein evidence of the possibly illicit activity persists for forensic use, long after the action itself has been concluded.

2. The method of claim 1 comprising receiving said signal from a detector responsive to image data.

3. The method of claim 1 comprising receiving said signal from a detector that includes a watermark detector.

4. The method of claim 1 comprising receiving said signal from a detector that includes a visible structure detector.

5. The method of claim 1 comprising receiving said signal from a hybrid watermark/visible structure detector.

6. The method of claim 1 comprising receiving said signal from a detector that includes a detector of a predetermined pattern characteristic of a banknote.

7. The method of claim 1 comprising receiving said signal from a detector associated with a printer.

8. The method of claim 1 comprising receiving said signal from a detector associated with a scanner.

9. The method of claim 1 comprising receiving said signal from a detector associated with software used with a computer.

10. The method of claim 1 comprising receiving said signal from a detector associated with driver software for a peripheral device.

11. The method of claim 1 comprising receiving said signal from a graphics-related executable running on said computer system.

12. The method of claim 1 comprising receiving said signal from a detector associated with an operating system.

13. The method of claim 1 comprising receiving said signal from a detector associated with an internet browser.

14. The method of claim 1 comprising receiving said signal from a network adapter.

15. The method of claim 1 comprising receiving said signal from an interface port.

16. The method of claim 1 in which the forensic tracer data includes data selected from the group consisting of: data identifying the date of said activity, data identifying the serial number of the computer system, data identifying the serial number of a system component, data identifying a user of the computer system, data identifying a file, data indicating the nature of the event detected, data indicating the status of the computer system, data from a registry database, data relating to an external network connection, and data derived from a digital watermark payload.

17. The method of claim 16 in which the forensic tracer data includes at least two data selected from said group.

18. The method of claim 16 in which the forensic tracer data includes at least three data selected from said group.

19. The method of claim 1 comprising storing the forensic tracer data by appending same to a file stored in said non-volatile data store.

20. The method of claim 1 comprising storing the forensic tracer data in a system registry associated with the computer system.

21. The method of claim 1 in which the computer system includes an external interface, and the method includes storing the forensic tracer data on a remote device by transmitting same to the remote device through the external interface.

22. The method of claim 1 comprising bypassing a computer system file system when storing the forensic tracer data, wherein the data is not reflected in a file directory listing of the computer system.

23. The method of claim 1 comprising encrypting said forensic tracer data.

24. The method of claim 1 comprising steganographically encoding said forensic tracer data.

25. The method of claim 1 including steganographically encoding said forensic tracer data within data stored in the non-volatile data store.

26. The method of claim 1 in which said illicit activity is processing image data corresponding to a banknote.

27. The method of claim 1 comprising storing said forensic tracer data redundantly in said non-volatile data store.

28. The method of claim 1 comprising storing at least some of said forensic tracer data after a delay interval.

29. The method of claim 1 which includes generating said forensic tracer data redundantly.

30. The method of claim 1 which includes transmitting said forensic tracer data redundantly.

31. The method of claim 1 which includes storing said forensic tracer data transparently.

32. The method of claim 1 which includes storing said forensic data inconspicuously.

33. A computer storage medium having instructions thereon causing a computer to inspect one or more non-volatile data stores associated with the computer searching for covert tracer data, said covert tracer data indicating possible use of the computer for an illicit activity, and producing output data indicating the results of said inspection.

34. A computer system comprising a processor and a non-volatile memory, the non-volatile memory including recognition data by which a predetermined image can be recognized, the system further including a detector that uses said recognition data to detect presence of data corresponding to said predetermined image in the computer system, the system further including means for storing an audit trail memorializing said detection.

35. A method of processing image data to screen for banknote images comprising, in the order stated:

(a) performing a first analysis on the image data;

(b) if the first analysis indicates the image data does not correspond to a banknote, skipping steps (c) – (e)

(c) performing a second analysis on the image data;

(d) if the second image analysis indicates the image data does not correspond to a banknote, skipping step (e); and

(e) flagging the image data as corresponding to a banknote.

36. The method of claim 35 that includes performing one or more additional analyses between steps (d) and (e), and skipping subsequent analyses if any of said additional analysis indicates the image data does not correspond to a banknote.

37. The method of claim 35 in which at least one of the analyses employs the Hough transform.

38. The method of claim 35 in which the first analysis is based on a rotationally invariant feature.

39. Apparatus for processing image data comprising:

a steganographic watermark detector responsive to a steganographic watermark that is characteristic of a security document; and

a pattern recognition detector responsive to a visible structure that is characteristic of a security document.

40. A photocopier according to claim 39.

41. A scanner according to claim 39.

42. A printer according to claim 39.

43. The apparatus of claim 39 that further includes an output having a signal that changes state when either of said detectors detects image data corresponding to a security document.

44. The apparatus of claim 43 further comprising a non-volatile memory for storing forensic tracer data in response to said signal.

45. A method of flagging image data as corresponding to a security document, comprising:

loading at least a portion of the image data into a memory;

analyzing the image data in the memory for the presence of a steganographic watermark indicative of a security document; and

analyzing the image data in the memory for the presence of a visible structure indicative of a security document.

46. The method of claim 12 that further includes interfering with reproduction of the image data if either of said analyzing steps indicates that the image data corresponds to a security document.

47. A method of flagging image data as corresponding to a security document, comprising:

re-registering the image data;

analyzing the re-registered image data for the presence of a steganographic watermark indicative of a security document; and

analyzing the re-registered image data for the presence of a visible structure indicative of a security document.

48. The method of claim 46 that further includes interfering with reproduction of the image data if either of said analyzing steps indicates that the image data corresponds to a security document.

49. The method of claim 46 in which the re-registering includes determining a scaling or rotation factor by reference to detection of calibration data embedded within the image data, and compensating for said determined factor.

50. The apparatus of claim 43 further comprising means for storing an audit trail memorializing detection of a security document.

51. The method of claim 45 that includes generating forensic tracer data redundantly, transmitting said forensic tracer data redundantly, and storing said forensic tracer data both transparently and inconspicuously, all in response to detection of either said steganographic watermark or said visible structure.

52. The method of claim 51 in which the forensic tracer data includes data selected from the group consisting of: data identifying the date of an activity, data identifying the serial number of a computer system, data identifying a serial number of a system component, data identifying a user of the computer system, data identifying a file, data indicating the nature of a detected event, data indicating the status of the computer system, data from a registry database, data relating to an external network connection, and data derived from a digital watermark payload.

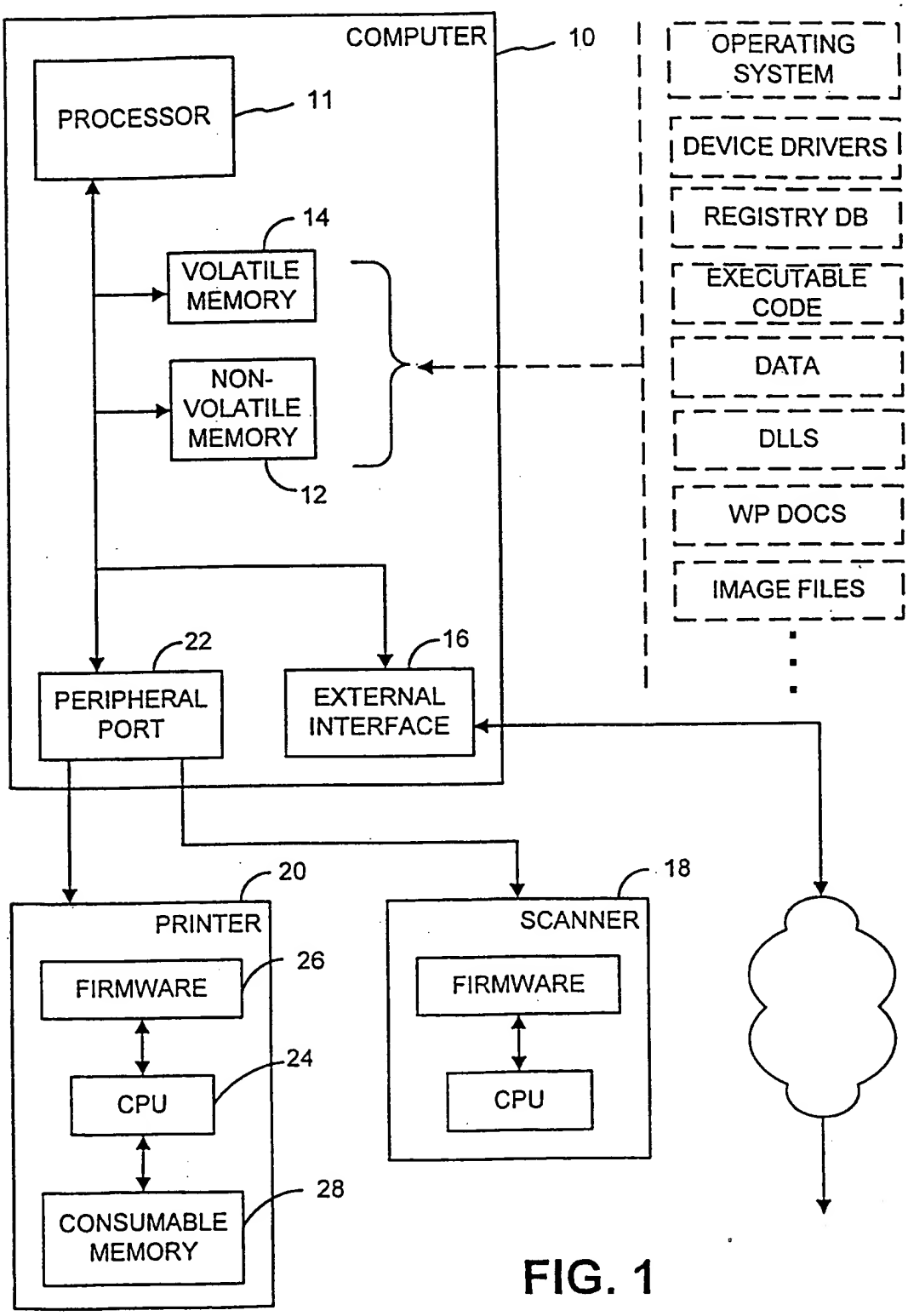

COMPUTER
10
PROCESSOR
11
14
VOLATILE MEMORY
NON-VOLATILE MEMORY
12
OPERATING SYSTEM
DEVICE DRIVERS
REGISTRY DB
EXECUTABLE CODE
DATA
DLLS
WP DOCS
IMAGE FILES
22
PERIPHERAL PORT
16
EXTERNAL INTERFACE
20
PRINTER
FIRMWARE
26
CPU
24
CONSUMABLE MEMORY
28
18
SCANNER
FIRMWARE
CPU

FIG. 1

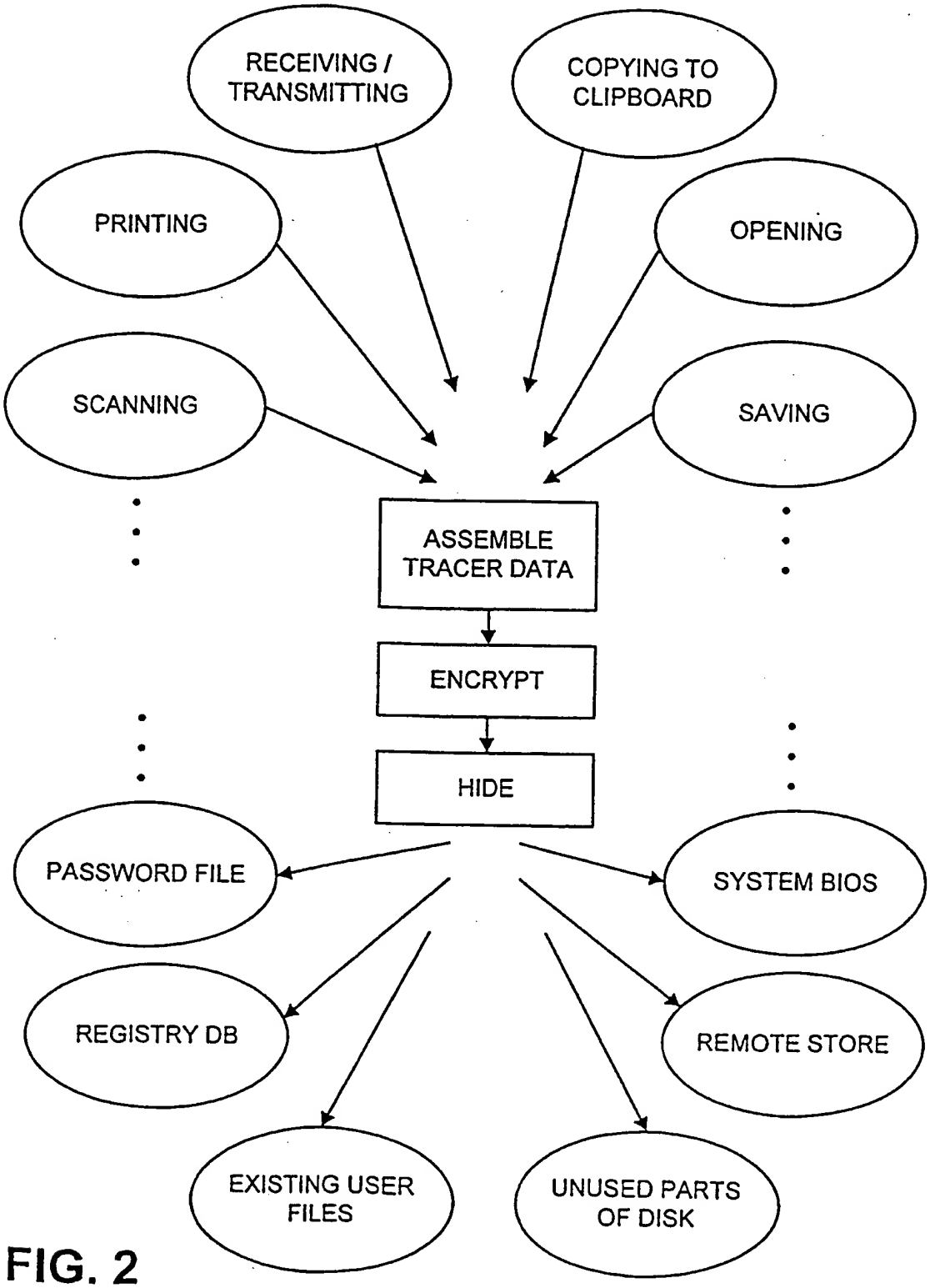

RECEIVING / TRANSMITTING
COPYING TO CLIPBOARD
PRINTING
OPENING
SCANNING
SAVING
ASSEMBLE TRACER DATA
ENCRYPT
HIDE
PASSWORD FILE
SYSTEM BIOS
REGISTRY DB
REMOTE STORE
EXISTING USER FILES
UNUSED PARTS OF DISK

FIG. 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/25375

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 1/00; G06K 9/00
US CL :713/200; 382/100, 135

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 713/185, 187, 200; 705/57; 714/45; 382/100, 135, 137, 227, 232, 281; 356/71; 380/54, 55

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,377,269 A (HEPTIG et al) 27 December 1994, see the final 5 lines of the abstract; column 2, lines 47-53; column 3, lines 55-58; column 11, lines 52-61; column 12, lines 14-22; column 15, lines 49-59; and Figures 9b and 12b.	1 and 7-34
X	US 5,652,802 A (GRAVES et al) 29 July 1997, see column 22, lines 13-67 and Figures 15A and 15B.	35-38
A,P	US 5,974,548 A (ADAMS) 26 October 1999, see the entire document.	1-34 and 39-52
A	US 5,483,658 A (GRUBE et al) 09 January 1996, see the entire document.	1-34

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
09 FEBRUARY 2000

Date of mailing of the international search report
29 FEB 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231

Facsimile No. (703) 305-3230

Authorized officer
ANDREW W. JOHNS
For Regenia Jagan

Telephone No. (703) 305-3800

Form PCT/ISA/210 (second sheet)(July 1992) ★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/25375

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,557,742 A (SMAHA et al) 17 September 1996, see the entire document.	1-34
A	US 5,483,602 A (STENZEL et al) 09 January 1996, see the entire document.	35-52
A	US 5,678,155 A (MIYAZA) 14 October 1997, see the entire document.	35-38
A,P	US 5,838,814 A (MOORE) 17 November 1998, see the entire document.	39-52

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/25375

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/25375

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be searched, the appropriate additional search fees must be paid.

Group I, claim(s)1-34, drawn to detecting and tracing illicit activity in a computer system.
Group II, claim(s) 35-38, drawn to detecting banknotes.
Group III, claim(s) 39-52, drawn to detecting steganographic watermarks.

The inventions listed as Groups I, II and III do not relate to a single inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: The claims of groups II and III do not set forth any limitations directed towards detecting or tracing illicit activities on a computer system as set forth in group I. The claims of groups I and III do not set forth any limitations directed towards the two stage banknote detection required in group II. Finally, none of the claims of groups I or II sets forth any limitations directed towards detecting steganographic watermarks, as required by the claims of group III.